CLAIMS

What is claimed is:

1. A system, comprising:

a local area network (LAN) having at least one host device, the at least one host device having software to perform anti-virus scanning;

a communication module to communicate anti-virus protection information for the at least one host device to the access module; and

an access module couple to the LAN to maintain a policy regarding anti-virus protection for the LAN and manage anti-virus protection scanning performed by the at least one host device, the access module to exchange anti-virus protection information with the one host device using the communication module of the host.

2. The system defined in Claim 1 wherein the communication module is part of the at least one host device.

3. The system defined in Claim 1 wherein the access module sends at least one command to the at least one host device via the communication module.

4. The system defined in Claim 3 wherein the at least on command comprises a command selected from a group comprising: a command to request status

of the anti-virus protection of the at least on host device, a command to have the at least one host to update the anti-virus protection, a command to uninstall the anti-virus protection, and a command to check a specific file or directory.

5. The system of claim 1, wherein a system administrator sets a range of compliance for the anti-virus protection policy.

6. The system of claim 5, wherein the Internet access module denies access to the Internet to the at least one host device if not in the range of compliance.

7. The system of claim 1, wherein the access module enforces and maintains the anti-virus protection policies for more than one host device.

8. The system of claim 7, wherein the anti-virus protection policies differ between host devices on the LAN.

9. The system of claim 1, wherein the host device communicates a version number of the anti-virus protection software on the host device to the access module.

10. The system of claim 9, wherein the host device communicates the version number using an out-of-band protocol.

11. The system of claim 9, wherein communications using the out-of-band protocol are encrypted.

12. The system of claim 1, wherein the host device communicates a time stamp indicating when the anti-virus protection software was last updated on the host device to the access module

13. The system defined in Claim 12 wherein the host device commutes the time step using an out-of-band protocol.

14. The system of claim 1, wherein the access module initiates an update in anti-virus protection for the host-device.

15. The system defined in Claim 14 wherein the access module initiates the update using the out-of-band protocol.

16. The system of claim 1, wherein the host device reports a problem with a virus to the Internet access module.

17. The system of claim 1, wherein the access module is a live firewall.

18. The system of claim 1, wherein the access module is a proxy server.

19. The system of claim 1, wherein the access module is a router.

20. The system of claim 1, wherein the access module is a modem.

21. The system of claim 1, wherein the access module is a gateway.

22. The system of claim 1, wherein the access module is an application server.

23. A method, comprising:

connecting a local area network to an Internet via an Internet access module;

connecting a host device to the Internet via the local area network; and

using the Internet access module to enforce a policy for anti-virus protection on the host device.

24. The method of claim 22, further comprising connecting the host device with the Internet access module via an out of band protocol.

25. The method of claim 23, further comprising communicating a version number of the anti-virus protection on the host device to the Internet access module over the out of band protocol.

26. The method of claim 23, further comprising communicating a time stamp

indicating when the anti-virus protection was last updated on the host device to the Internet access module over the out of band protocol.

27. The method of claim 23, further comprising initiating an update in anti-virus protection for the host-device over the out of band protocol.

28. The method of claim 23, further comprising encrypting the out of band protocol.

29. The method of claim 22, further comprising connecting more than one host device to the local area network.

30. The method of claim 28, further comprising using the Internet access module enforces and maintains the anti-virus protection policies for more than one host device.

31. The method of claim 29, wherein the anti-virus protection policies differ between host devices.

32. The method of claim 22, further comprising applying a range of compliance for the anti-virus protection policy set by a system administrator.

33. The method of claim 31, further comprising denying access to the Internet to those host devices not in the range of compliance.

34. The method of claim 32, further comprising:

removing the range of compliance upon notice of a virus alert

denying the host device access to the web if the device does not have the most current version of anti-virus protection.

35. The method of claim 22, further comprising the host device is checked repeatedly to make sure the anti-virus protection is not disabled.

36. The method of claim 22, further comprising reporting a problem with a virus to the Internet access module.